This listing of claims will replace all prior versions, and listings, of claims in the application:

Claim 1 (Currently Amended): An apparatus for recording information ~~image or other data in real time~~, comprising:

a capture device for capturing the ~~image or other~~ information;

a local verification device for indelibly marking the captured ~~image or other~~ information with the actual date[[,]] and time[[,]] of the capture of the information, and the actual location information defining the location of said capture device at the time of capture of the information, such that such date, time and location information becomes part of the captured information as bound captured information;

a signature device for creating owner information ~~and information~~ identifying the creator and owner of the bound captured information and ~~data~~; placing the bound captured information in combination with the owner information in a predefined secure transmission file formatted to be uniquely recognized by a secure storage facility;

a transmitter for transmitting the ~~locally verified captured image or other information~~ secure transmission file ~~in real time~~ to [[a]] the secure storage facility, wherein the secure storage facility is operable to store bound captured information in association with the owner; and

~~said capture device receiving and verifying~~ the secure storage facility generating an acknowledgment of the receipt of the transmitted ~~locally verified captured image or other information~~ secure transmission file to the secure storage facility, wherein the acknowledgment has associated therewith at least a portion of the information contained within the transmitted secure transmission file.

Claim 2 (Currently Amended): The apparatus of Claim 1 wherein the captured information comprises a captured image and where [[the]] said capture device is a digital camera.

Claim 3 (Currently Amended): The apparatus of Claim 1 wherein the captured information comprises a captured image and where [[the]] said capture device is a video camera.

Claim 4 (Currently Amended): The apparatus of claim 1 where said local verification device comprises a geographical position and time-of-day determination (GPS) receiver.

Claim 5 (Currently Amended): The apparatus of Claim 1, and further comprising ~~a secure signature authority~~ certifier for transmitting a representation of the locally verified captured ~~image or other~~ information to a Certification Authority (CA) as a trusted third party for certification thereof and return of a certificate of authority, which is merged with and becomes a part of said ~~locally verified~~ captured ~~image or other~~ information.

Claim 6 (Currently Amended): The apparatus of Claim 1, and further comprising an encryption device for encrypting ~~the locally verified~~ the bound captured ~~image or other~~ information ~~prior~~ prior to transmission thereof with a first level of encryption to provided an encrypted file, which first level of encryption constitutes a symmetrical encryption algorithm that has a secret key available only to the owner and wherein the encrypted file is placed in combination with the owner information in the predefined secure transmission file, wherein the secure storage facility is operable to store only the encrypted file in association with the owner.

Claim 7: (New) The method of Claim 6, wherein the first level of encryption comprises a hash of a unique ID associated with said capture device to create a private key with no associated public key, wherein the owner has possession of the private key.

Claim 8: (New) The method of Claim 6, wherein said encryption device is operable to wrap the encrypted file with a second layer of encryption that is comprised of an asymmetrical encryption layer that has a public and private key owned by the owner, such that the owner is the only one that can encrypt the encrypted file with the second layer of encryption, and wherein encrypted file wrapped with the second layer of encryption is placed in combination with the owner data in the predefined secure transmission file, such that the secure storage facility can recognize the owner and then determine the associated public key to unwrap the second layer of encryption and store the encrypted file.

Claim 9: (New) The method of Claim 8, wherein the encrypted file is passed through a message authentication algorithm by said encryption device to provide a hash of the encrypted file, the hash of the encryption fie then combined with the encrypted file and place in combination with the owner information in the secure transmission file and wherein the secure storage facility is operable to store only the combination of the encrypted file and the hashed encrypted file in association with the owner and, wherein the secure storage facility is operable to pass the received encrypted file through the same message authentication algorithm that created the received hash of the received encrypted file to provide a new hash of the received encrypted file and then compare the newly created hash with the received hash and, if they compare true, store at least the received encrypted file in association with the owner.

Claim 10: (New) The method of Claim 8, wherein the encrypted file after wrapping with the second layer of encryption by said encryption device is wrapped with a third encryption layer that is comprised of an asymmetrical encryption layer that has a public and private key owned by the secure storage facility, such that the secure storage facility is the only one that can decrypt the third layer of encryption to expose the encrypted file wrapped with the second layer of encryption.

Claim 11: The method of Claim 1, wherein the secure transmission file is created and transmitted at substantially the same time as the time of capture.

Claim 12 (New): An apparatus for recording images for secure transmission to a secure storage facility, comprising:

a capture device for capturing a native image and which said capture device is owned and controlled by an owner;

a local verification device for indelibly marking the captured native image with the actual date and time of the capture of the information, and the actual location defining the location of said capture device at the time of capture of the native image, such that such date, time and location information becomes an integral part of the captured native image as a bound image file;

a signature device for creating owner information identifying the creator and owner of the bound image file and placing the bound image file in combination with the owner data in a predefined secure transmission file formatted to be uniquely recognized by a secure storage facility;

an encryption device for encrypting the bound image file with a first level of encryption to provided an encrypted file, which first level of encryption constitutes a symmetrical encryption algorithm that has a secret key available only to the owner and wherein the encrypted file is placed in combination with owner information identifying the creator and owner of the bound image file in a predefined secure transmission file formatted to be uniquely recognized by a secure storage facility, wherein the secure storage facility is operable to store only the encrypted file in association with the owner;

a transmitter for transmitting the secure transmission file to the secure storage facility, wherein the secure storage facility is operable to store bound captured information in association with the owner; and

the secure facility generating an acknowledgment of the receipt of the transmitted secure transmission file to the secure storage facility, wherein the acknowledgment has associated therewith at least a portion of the information contained within the transmitted secure transmission file.

Claim 13 (New): The apparatus of Claim 12, and further comprising a certifier for transmitting a representation of the locally verified captured native image to a Certification Authority (CA) as a trusted third party for certification thereof and return of a certificate of authority, which is merged with and becomes a part of said locally verified captured native image.

Claim 14: (New) The method of Claim 12, wherein the first level of encryption comprises a hash of a unique ID associated with said capture device to create a private key with no associated public key, wherein the owner has possession of the private key.

Claim 15: (New) The method of Claim 12, wherein said encryption device is operable to wrap the encrypted file with a second layer of encryption that is comprised of an asymmetrical encryption layer that has a public and private key owned by the owner, such that the owner is the only one that can encrypt the encrypted file with the second layer of encryption, and wherein encrypted file wrapped with the second layer of encryption is placed in combination with the owner data in the predefined secure transmission file, such that the secure storage facility can recognize the owner and then determine the associated public key to unwrap the second layer of encryption and store the encrypted file.

Claim 16: (New) The method of Claim 15, wherein the encrypted file is passed through a message authentication algorithm to provide a hash of the encrypted file, the hash of the encryption file then combined with the encrypted file and placed in combination with the owner information in the secure transmission file and wherein the secure storage facility is operable to store only the combination of the encrypted file and the hashed encrypted file in association with the owner and, wherein the secure storage facility is operable to pass the received encrypted file through the same message authentication algorithm that created the received hash of the received encrypted file to provide a new hash of the received encrypted file and then compare the newly created hash with the received hash and, if they compare true, store at least the received encrypted file in association with the owner.

Claim 17: (New) The method of Claim 15, wherein the encrypted file after wrapping with the second layer of encryption by said encryption device is wrapped with a third encryption layer that is comprised of an asymmetrical encryption layer that has a public and private key owned by the secure storage facility, such that the secure storage facility is the only one that can decrypt the third layer of encryption to expose the encrypted file wrapped with the second layer of encryption.

Claim 18: The method of Claim 12, wherein the secure transmission file is created and transmitted at substantially the same time as the time of capture.